BluStar 8000i Desktop Media Phone & BluStar for Conference Room

INSTALLATION INSTRUCTIONS

AASTRA

Copyright

© Copyright Aastra Technologies Limited, 2014. All rights reserved.

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Aastra shall have no liability for any error or damage of any kind resulting from the use of this document.

1 General

This document is valid for Aastra BluStar 8000i and Aastra BluStar for Conference Room, when installing this telephone in an MX-ONE environment.

1.1 Scope

This document describes how to install and configure the BluStar 8000i and BluStar for Conference Room, in an MX-ONE Telephony Server environment, see *Installation Instructions for Aastra 6700i SIP Terminals for MX-ONE*.

For information that is common for BluStar 8000i, BluStar for Conference Room and Aastra 6700i, Installation Instructions for Aastra 6700i SIP Terminals for MX-ONE.

For general installation information that is not unique for a MX-ONE environment, there is a reference to the Aastra BluStar 8000i Desktop Media Phone / BluStar for Conference Room, SIP Call Server Administrator Guide, which is platform independent.

For information how to use the phones, Aastra BluStar 8000i and Conference Room, User Guide, see Aastra BluStar 8000i Desktop Media Phone, User Guide.

1.2 Glossary

Some expressions in this document follow the expressions used in MX-ONE, which can differ from the expressions used in the Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

Table 1 Expressions used in MX-ONE and BluStar Admin Guide

MX-ONE	BluStar Admin. Guide
MNS (Monitored extensions)	BLF (Busy Lamp Field)
Software server	Configuration server
TNS (Telephony Name Selection)	Speed dial
Corporate directory	Global directory

Below is a table explaining some abbreviations in this document.

Table 2 Abbreviations

Abbreviation	Explanation
FTP	File Transfer Protocol
IPP	IP Phone SW Server Configuration Management Application for Windows
CSV	Comma Separated Value

1.3 Environmental Requirements

Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

2 Cabling

Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

3 Power Equipment

Both the 8000i telephone and the Conference Room unit are powered from:

- AC/DC adaptor 3A-603DB12.

For the complementary units to BluStar for Conference Room:

- Aastra HD 610 camera, powered from 87-00062AAA-A
- Remote control to the HD 610 camera is powered by 2 AAA standard batteries
- Aastra Wireless Keyboard used for the Conference Room unit is powered by 2 AAA standard batteries

For the Aastra S850i audio unit, please that units documentation.

4 Earthing and Grounding

Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

5 Prerequisites

5.1 Licences

To be able to use the BluStar 8000i phone or the BluStar for Conference Room, one video license in MX-ONE is mandatory. The video license is connected to the extension number and up to four SIP terminals can be connected to the extension number. For more information, see command description for Generic Extension.

One license for generic extension and one license for the IP extension are needed.

5.2 PIN code

An IP extension that will be used with BluStar 8000i and BluStar for Conference Room must have a PIN code (Individual Authorization code) initiated in MX-ONE in order to be registered to MX-ONE and authenticated towards BluStar Configuration in Manager Telephony System (MTS).

If BluStar Configuration is not used for authentication, PIN code is not mandatory, but recommended.

.

6 Setting up the Software Server

There are some alternatives to host the software and the configuration files:

- IP Phone SW Server Configuration Management Application for Windows (CXC 109 0055/1) also called IPP. This application is using a Tomcat http server.
- HTTP server, for example Apache or IIS.
- FTP server, for example Filezilla.

6.1 IP Phone SW Server Configuration Management Application

The recommendation is to use the IPP as software server. The advantage is to get support from MX-ONE Management Applications (MTS) to create the configuration files aastra.cfg and 8000i.cfg. MTS stores the configuration files on the IPP server.

The configuration file 8000icr.cfg used for BluStar for Conference Room is not managed by MTS, but can be stored and administrated on the IPP server.

(Since the contents of the 8000icr.cfg file are identical to that of the 8000i.cfg, then the file created by MTS for the BluStar 8000i may be copied and renamed to 8000icr.cfg).

For information how to set up the IPP Tomcat server, see Installation Instructions for Aastra 6700i SIP Terminals for MX-ONE.

6.2 Using an HTTP / FTP Server

One alternative is to use an HTTP server (not IPP) but in this case the configuration files aastra.cfg and 8000i.cfg/8000icr.cfg has to be edited manually.

If an HTTP server is already used as software server for the other IP phones, this option can be useful.

6.2.1 Setting up the HTTP / FTP server

For a description of the different software files and of the recommended directory structure, see 9.1 Software files on page 22.

Follow the steps below:

- If HTTP/HTTPS is used to push the <user>.cfg and <user>_local.cfg to the server, the following two files need to be in a folder specified in the parameter user configuration URL in the 8000i.cfg/8000icr.cfg file:
  - upload.html
  - upload_file.php

These files are available via Service Plaza Knowledge Database. PHP has to be in-stalled on the server and the folder has to allow writing.

- Store the software files under the folder <version> with the files 8000i.ver, upgradevipr.tar and UI.xml.
- The aastra.cfg file has to be available on the HTTP server. If Aastra 6700i SIP phones are used in the system the BluStar 8000i and BluStar for Conference Room will use the same aastra.cfg file. If this file has to be created, it shall be based on the template for aastra.cfg stored in MX-ONE under /etc/opt/eri_sn/aastraSIP-phones.
- The model specific configuration file is called 8000i.cfg/8000icr.cfg. A template file for BluStar 8000i is stored in MX-ONE under /etc/opt/eri_sn/aastraSIPphones. The same template file can be used for the BluStar for Conference Room. For a description of parameters to be filled in, see 8.1.2 Manual handling of 8000i.cfg and aastra.cfg on page 15.
- Picture Sample*.png files. Various sample png files for picture identity. For more information see Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

7 Manage the Configuration Files in Manager Telephony System

This section describes the support that MTS can give to create the different configuration files.

7.1 The Configuration Files for BluStar 8000i

The following configuration files for BluStar 8000i are handled via MTS:

- aastra.cfg: common with the Aastra 6700i SIP phones and should be created from Manager Telephony System (MTS), see 7.3 IP Phone Configuration File in MTS on page 12.
- 8000i.cfg: the model specific configuration file should be created from Manager Telephony System, see 7.3 IP Phone Configuration File in MTS on page 12.

The following files are handled via BluStar Configuration:

- <user>.cfg: the file with user unique call server related data is created automatically by BluStar Configuration in MTS when the user logs on the phone after the first registration of the phone towards MX-ONE.
- <user>_local.cfg: the file contains free seating related data for the user. It is created automatically by the BluStar 8000i phone and does not have to be touched by the system administrator. It is stored via BluStar Configuration, see 8.2.1 Automatically Generated <user>.cfg by BluStar Configuration on page 18.

When managing the configuration files for BluStar 8000i in MTS, select the IP Phone family = aastra67xxi, where also BluStar 8000i is handled.

7.2 The Configuration Files for BluStar for Conference Room

The following configuration files for BluStar for Conference Room are handled via MTS:

- aastra.cfg: common with the Aastra 6700i SIP phones and should be created from Man-ager Telephony System (MTS).

The following files are handled via BluStar Configuration:

- 8000icr.cfg: the model specific configuration file is not managed via MTS, instead a 8000i.cfg file can be created by MTS and thereafter copied and renamed to 8000icr.cfg.
- <user>.cfg: the file with user unique call server related data is created automatically by BluStar Configuration in MTS when the user logs on the phone after the first registration of the phone towards MX-ONE.
- <user>_local.cfg: the file contains free seating related data for the user. It is created au-tomatically by the BluStar 8000i phone and does not have to be touched by the system administrator. It is stored via BluStar Configuration.

7.3 IP Phone Configuration File in MTS

MX-ONE Manager Telephony System (MTS) shall be used when creating or changing the aastra.cfg and the model specific configuration files. The information regarding parameters is available in the online help for MX-ONE Manager Telephony System. The picture below shows an example of the page in the IP Phone Configuration File task in MTS:

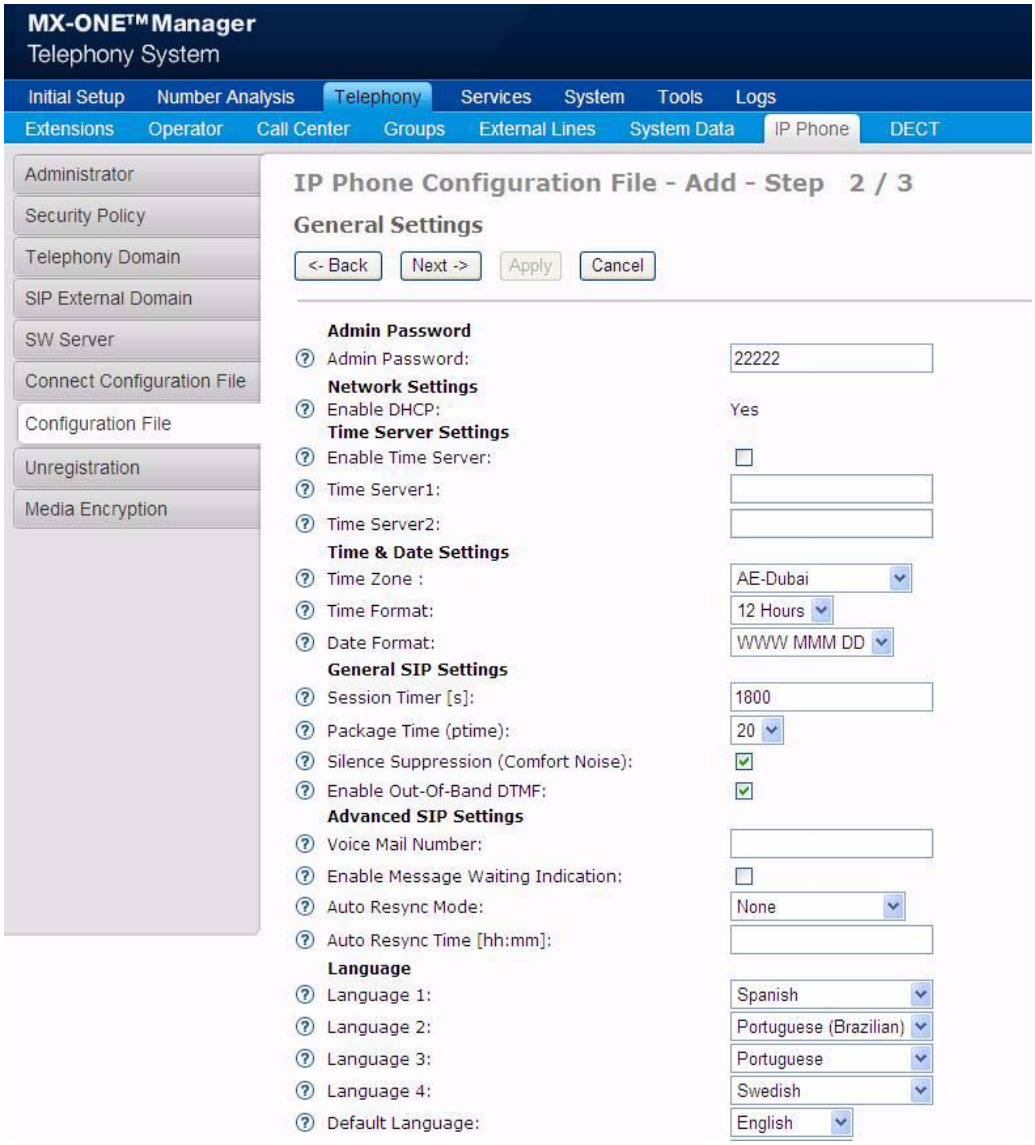

Figure 1: IP Phone Configuration File in MTS

Note: MTS requires that the IP Phone SW Server Configuration Management Application is installed on the IP Phone SW Server, please section 6 Setting up the Software Server on page 9

7.4 Create a Configuration File

The procedure to create a new configuration file is:

- Log in to MX-ONE Manager Telephony System.
- Go to **Telephony** > **IP Phone** > **Configuration file**. Press **Add new** to open the new configuration file.

Select **Aastra 67xxi** family, where BluStar 800i is also handled, and enter the data into the configuration file which is automatically stored under the correct directory in the IP Phone Software Server when pressing **Apply**.

- To force the telephones to fetch the new configuration file there are a number of cases:
  - If the telephones are not started yet: connect the power and the telephones will fetch the new configuration file.
  - The telephones will after less than 24 hours automatically fetch the new configuration file and if necessary download a new firmware.
  - Restart the telephones manually.

7.5 Changing an Existing Configuration File

The existing configuration file can be updated using the **MX-ONE Manager Telephony System**.

The following procedure shall be used when the configuration file shall be changed:

1. Log in to MX-ONE Manager Telephony System and select:

   Telephony > **IP Phone** > **Configuration file**

2. Take a backup copy of the existing configuration file by pressing the backup icon.
3. Use the **Change** icon to view the configuration file. When the adaptation of the file is completed, it is automatically stored under the **aastra67xxi** directory in the IP Phone Software Server.
4. Copy and re-name the 8000i.cfg file to 8000icr.cfg.
5. To load the updated file into the phone: restart BluStar 8000i/BluStar for Conference Room by touching the **app menu** and select **log off and restart**.

7.6 More MTS Features

For a descriptions of more features for handling the configuration files, *Installation Instructions for Aastra 6700i SIP Terminals for MX-ONE*.

8 How to Start a New Phone

The configuration files must be adapted to the local network.

Most settings in the phone can be controlled by the configuration files, available on the software server. When the phone is powered up, the configuration files are downloaded to the phone from the software server.

For a detailed description of the different software files, 9.1 Software files on page 21

8.1 Installing aastra.cfg and 8000i.cfg/8000icr.cfg configuration files

8.1.1 Using MTS

For **aastra.cfg** and **8000i.cfg /8000icr.cfg** the following is valid:

1. The **aastra.cfg** file: If this file does not already exist, the system administrator shall create the file by using the Configuration File task in MTS.
2. Create the model specific **8000i.cfg/8000icr.cfg** file by using the Configuration File task in MTS.

   Select the IP Phone family = **aastra67xxi**, where also BluStar 8000i is handled.
3. Restart the BluStar8000i by touching the **app menu** and select **log off and restart** to make the phone read the configuration files.

For the 8000icr.cfg the following is valid:

1. Create the a 8000i.cfg file as normal using MTS, thereafter make a copy of the file and re-name to 8000icr.cfg and thereafter continue as for BluStar 8000i.

8.1.2 Manual handling of 8000i.cfg and aastra.cfg

If MTS cannot be used for creating these configuration files**,** use the template files, which are stored in Telephony Server in the folder /etc/opt/eri_sn/aastraSIPphones.

The following procedure describes how to install the configuration files and the unique parameters for Aastra BluStar 8000i/BluStar for Conference Room:

1. The **aastra.cfg** and the **8000i.cfg** files must be available on the software server.
2. In **8000i.cfg:** Below is a list with the most important parameters:
    - **user config url:** the address to BluStar Configuration in MTS or to the configuration server where the **<user>.cfg** and **<user>_local.cfg** files are stored. The parameter value shall normally be:
      http://<address to MTS webserver>/BluStarConfigServer/userConf

      Replace http with https in the beginning of the string, if https shall be used.
    - **update url:** the address to the software server where the software for the phone is stored.
    - **!pbx mode**: if the phone shall be used in SIP Call Server mode or BAS mode. Shall normally be set to 1, when used with MX-ONE. If both BAS and call server terminals shall be used in the same network, the parameter shall be removed from this file and specified in the <mac>.cfg files.
    - **telephony integration url**: the URL that the phone calls to perform PBX integration, for features like DND, Call Forward etc. The parameter value shall normally be:

      http://$$PROXYURL$$:22222/8000i
    - **telephony integration use login credentials**: the phone will use userid and PIN code to authenticate towards the PBX integration server.
    - **enable user defined exchange contacts**: if the user shall be allowed to import his Microsoft Exchange® personal contacts.
    - **telephony integration needs sip registration:** indicates that the SIP registration status must be checked before sending a user request. Shall always be enabled in a MX-ONE environment.
    - **language name:** the language that shall be used in the 8000i terminals and Conference Room units, also12.4 Configuring Language Settings on page 28.
    - **tos rtp video:** type of service for the video rtp packets.
    - **user defined power savings schedule:** Parameters for defining the schedule for power saving, section 12.23 Power Saving on page 33.

- **directory 1**: the name of the global directory file that can be downloaded from the software server. Example: directory 1: //ftp/192.168.0.5/path/global.csv.
- **Enable user login**

  also section 12.16 Directories and Contacts on page 31.

If LDAP shall be used for access to the global directory, the following parameters are necessary and the recommendation is to include them in 8000i.cfg:

- **ldap name**: directory name
- **ldap server: username:password@ldapserver:port**

  The different parts of the parameter value are:

  –**username:** is used for authentication. Is optional and if it is not provided, anonymous connection will be used.

  –**password:** is used for authentication. Optional.

  –**ldapserver:** is mandatory.

  –**port**: ldap interface port. Optional. Default value is 389, but if active directory shall be used, the value is 3268.

  Examples: *ldap server: ldap.company.com*
  ldap server: user:password@ldap.company.com:3268
- **ldap base dn:dc=<domain1>,dc=<domain2>**

  Specify the ldap server base Distinguished Name (DN) or the top level of the directory tree. Usually if the company domain is company.com the base DN must be entered under the form “dc=company, dc=com”.
- **ldap use login credentials**: if the userid/password used to log in to the phone shall also be used for log in to ldap. Shall normally be off.
- **ldap use iso-8859-1 encoding:** specifies whether or not the LDAP directory uses ISO-8859-1 or UTF-8. When the parameter is enabled the terminal will transcode characters from ISO-8859-1 to the equivalent UTF-character.
- **ldap dn query mode:**
- **ldap search scope**:

For details Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference for Conference, SIP Call Server Administrator Guide.

3. Restart the BluStar8000i/BluStar for Conference Room by touching/tapping the **menu** and select **log off and restart.**

8.2 Installing the User Unique Configuration Files

The user unique configuration files can be generated automatically by BluStar Configuration in MTS or they can as an alternative be manually created.

8.2.1 Automatically Generated <user>.cfg by BluStar Configuration

There is a component distributed with MTS called BluStar Configuration where the user unique configuration file **<user>.cfg** is created automatically. BluStar Configuration stores also the **<user>_local.cfg** that the phone generates.

There is no user interface for BluStar Configuration, the only thing that the system administrator has to do is to define the parameter **user config url** in the 8000i.cfg/8000icr.cfg file.

First time the user logs on the phone, BluStar Configuration creates the **<user>.cfg** file and stores it under the folder /var/opt/eri_om/users in MX-ONE server 1. The **<user>_local.cfg** is stored there at log off.

Note: In the current version of BluStar Configuration, it is not possible to manually change any parameter in the **<user>.cfg** file, because it will be overwritten the next time the user logs on. If a parameter has to be changed for a user, BluStar Configuration cannot be used and the file has to be changed manually and stored in another location. In this case the url, to where to store the file, must be specified in a **<mac>** file (in the **user config url** parameter) for this terminal.
Change of PIN code as described in section 8.3.3 Change of PIN code on page 19*,* will then be no longer possible.

The alternative is to create all the files manually, 8.2.2 Manually created <user>.cfg on page 17.

8.2.2 Manually created <user>.cfg

If BluStar Configuration in MTS cannot be used for any reason, the **<user>.cfg** file must be created manually. Use the template file stored in MX-ONE in the folder /etc/opt/eri_sn/aastraSIPphones.

The following parameters are important:

- **sip auth name**: define the directory number
- **sip password:** define the PIN code if it is defined in MX-ONE.
- **sip user name:** define the directory number

- **sip screen name:** enter the name of the user
- **sip screen name 2**: define the directory number to be shown in the idle display.
- **sip proxy ip:** IP address to the MX-ONE server to which the phone sends the sip requests. The IP address shall be equal as in sip registrar ip.
- **sip registrar ip:** IP address to the MX-ONE server to which the phone sends the sip requests. The IP address shall be equal as in sip proxy ip.
- **directory 2**: the name of the user directory file that can be down-loaded from the software server. Example: directory 2: ftp//:192.168.0.5/path/67609.csv.

  also section 12.16 Directories and Contacts on page 31.

The file shall be stored on the software server. Enable read and write access on the FTP/HTTP server because the phone writes in the file at log off.

The phone creates the **<user>_local.cfg** file with personal settings for example call logs, favorites and speed dial data

The phone reads these two files when logging on to the phone and uses the values in **<user>.cfg** to be able to register towards MX-ONE.

Note: The file must be stored in UTF-8 format to get special characters.

For more details, Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

8.3 Log on / Log off

The **<user>.cfg** file is mandatory.

In order to make calls, access the personal settings and use all of the BluStar 8000i and BluStar for Conference Room features, the user must first log on the phone by entering the user name and password (not mandatory, below) or by using the fingerprint reader (BluStar 8000i only).

For a description how the set up the finger print reader on BluStar 8000i, Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide

Concerning the user identity and password the following expressions are used:

- to log on to the phone; here called phone user id and password.

- to register the phone towards MX-ONE; here called extension number and PIN code.

There are a couple of scenarios at log on:

- Using BluStar Configuration in MTS.
- Using an FTP or HTTP server.

The scenarios are described below.

When logging off the phone, the user will also be logged off from MX-ONE.

8.3.1 Log on/off using BluStar Configuration

When using BluStar Configuration in MTS to authenticate the log on and automatically create the **<user>.cfg** file, the phone user id is equal to the user's extension number and password is equal to the user's PIN code. BluStar Configuration authenticates with Telephony Server (the LDAP data base) that the number and PIN code are correct and in this case returns SIP data necessary for the the phone to then register towards MX-ONE.

In this case PIN code is mandatory.

8.3.2 Log on/off using an FTP or HTTP server

When using an FTP or HTTP server, the **<user>.cfg** file is already manually created and stored on the server. The phone user id and password are used for authentication towards the FTP/HTTP server. The **<user>.cfg** file is fetched and the extension number, PIN code and SIP data in this file are then used by the phone to register towards MX-ONE.

When the phone user id is entered but no password, anonymous user or one user defined in the configuration file is used for authentication towards the FTP/HTTP server. Syntax for the parameter in the 8000i.cfg/8000icr.cfg file:

user config URL: ftp://<ftpuser>:<ftppasswd>@<ftpserver>/<ftppath>

The user id of the phone is used for creating or getting the **<user>.cfg** file. This file is fetched and the extension number and PIN code in this file are used to register towards MX-ONE.

8.3.3 Change of PIN code

If BluStar Configuration is used, the following procedure must be followed when changing the PIN code:

- Log off the terminal to save the current changes.

- Log on the terminal using the existing PIN code.
- Change the PIN code with *74*old PIN*new PIN#
- Log off the terminal to save the new PIN code.
- Log on the terminal using the new PIN code.

If BluStar Configuration is not used the user cannot change the PIN code. The system administrator has to change the PIN code in MX-ONE and edit the **<user>.cfg** file.

9 Managing IP Phone SW

The directory structure for Aastra 6700i and Aastra BluStar8000i/BluStar for Conference Room on the software server is shown in the picture below.

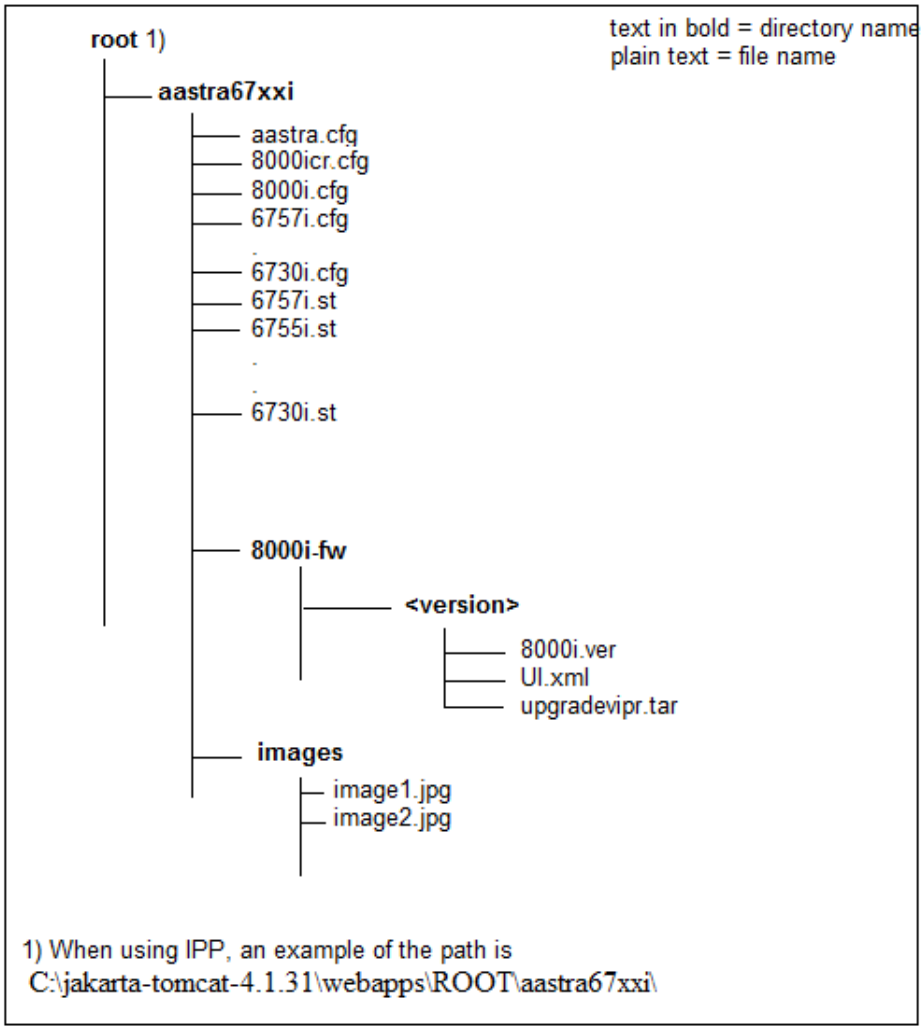

Figure 2: Directory structure

9.1 Software files

Below is a list with the different files that shall be stored on the software server.

If it is not possible to use MTS, to create the configuration files, these files must be created manually based on the templates stored in MX-ONE under **/etc/opt/eri_sn/aastraSIPphones/**.

<version>
BluStar software folder containing the files 8000i.ver/8000icr.ver, upgradevipr.tar and UI.xml. Example:

- **4.1.0-1116**

aastra.cfg
This file contains the configuration parameters for all Aastra6700i and BluStar8000i phones in the system. The configuration file has to be adapted for each installation.
This file may be created in IP Phone Configuration File task in Manager Telephone Server (MTS).

8000i.cfg
This file contains model specific information for 8000i. For example **PBX mode, configuration server URL** and **update URL**.

It will override the settings in aastra.cfg.

The file may be created in MTS.

8000icr.cfg

This file contains model specific information BluStar for Conference Room. For example **PBX mode, configuration server URL** and **update URL**.

It will override the settings in aastra.cfg.

The file cannot be directly created in MTS.

<mac>.cfg
This file is normally not used when the phone is used with MX-ONE. This file makes is possible to get unique parameter settings per telephone. **<mac>** represents the mac address of the phone. Example: **00085d1b5d8.cfg**
The settings in <mac>.cfg will override the settings in aastra.cfg and in 8000i.cfg8000icr.cfg.

No support in MTS/MP for this file.

images
Data base with images. These image files are also used by Aastra 6739i.

If BluStar Configuration is used, the following files are stored in MX-ONE in the folder **/var/opt/eri_om/users**:

<user>.cfg
This file contains user unique call server related data for the BluStar 8000i/BluStar for Conference Room user, for example directory number, PIN code, sip proxy and sip registrar address. This data

cannot be configured through BluStar 8000i/BluStar for Conference Room.

Example of the file name is **67609.cfg**.

This file is loaded when the user logs in.

The file is created automatically by BluStar Configuration each time the terminal is registered towards MX-ONE.

If it is not possible to use BluStar Configuration, this file must be created manually based on the template stored in MX-ONE under /etc/opt/eri_sn/aastraSIPphones/.

<user>_local.cfg

This file contains free seating related data for the user for example call logs and favorites. This data is configured by BluStar 8000i/BluStar for Conference Room and it is also the phone that creates the file. It should never be changed manually.

Example of the file name is **67609_local.cfg.**

This file is loaded when the user logs in and updated when the user logs off.

9.2 Installing the Firmware / Configuration files

When the phone is powered up, the phone fetches the configuration files from the software server and loads new firmware if the application file on the software server differs compared to the one stored in the phone.

To force the phones to restart and read the configuration files there is the following option:

Phone UI

- Touch the **app menu** and select **log off and restart.**

9.3 Viewing Software Version

It is possible to display the version of the software units.

Phone UI

- Select **app menu** and select **About**.

MX-ONE

- MX-ONE command: **extension_info** with the parameter **terminal-info**

10 Restart / Restore

There are the following options:

- Restart the phone. Can be used when settings shall be applied.
- Restore to factory default. The phone gets the same data as when leaving the factory and removes any saved directory files.

10.1 Restart

Phone UI

- Touch the **app menu** and select **log off and restart**

10.2 Autologin Upon Restart

BluStar 8000i/BluStar for Conference Room terminals can automatically log in to a specified default account upon a manual restart, forced restart or cold reboot.

These three processes can be defined as follows:

- **Manual restart** - user initiated (e.g. when a user selects the Restart button)
- **Forced restart** - software initiated but influenced by a user's action (e.g. when a user changes a terminal setting whereby the device requires a restart for the setting to take effect.
- **Cold reboot** - when a software upgrade has been initiated or when an interruption of power has occurred (e.g. power failure or power cycle).

Enabling the autologin feature is done in two steps:

- In the configuration files aastra.cfg, <model>.cfg, or <mac>.cfg files the following parameter shall be enabled:

  enable user autologin: 1

  The default value is disabled.

- The end user has to enable the feature for the specific terminal:
  - Log in to the BluStar device using the account you wish to configure as the autologin account

– Select the **App Menu** button
– Select the **Tools** button
– Select the **User Identity** button
– Select **Autologin, upon restart, for this account and device**
– Select **Done**

10.3 Restore to Factory Default

Phone UI

- Touch the **app** menu key > **tools** menu key > **utilities** menu key > **reset to factory default**

  The following message appears: *“Do you really want to log off and reset to factory default?”*

- Press **Reset.**

11 Entering Administrator Mode

There is no administrators mode.

12 Configuring the Unit

This chapter describes how to configure some of the features in the phone from the phone menus.

This chapter also covers the configuration via the configuration files, **aastra.cfg**, **8000i.cfg/8000icr.cfg** or **<mac>.cfg**.

The parameters can be set in any of these configuration files, but in this section it is the recommended placing that is described. If one parameter occurs in several configuration files, it is always the last read parameter value that the telephone uses.

For a description of the syntax of the parameters, Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

12.1 Settings mode

To set data in the phone touch the **app** menu key > **tools** menu key and select one option in the most upper tab row. For more detailed information the Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

12.2 LLDP-MED

The terminal has support for Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). This can for example be used to get:

- The emergency location identification number (ELIN). For more information *Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide*.
- The VLAN identity. For more information *Installation Instructions for Aastra 6700i SIP Terminals for MX-ONE*.

12.3 Using Virtual LAN (VLAN)

By configuring specific VLAN parameters, the BluStar 8000i/BluStar for Conference Room, has the capability of adding and removing tags, and processing the ID and priority information contained within the tag.

The following configuration alternatives are available:

- **LLDP-MED**. section 12.2 LLDP-MED on page 27
- **DHCP option 43**. section 18.3 DHCP Settings for Option 43 and 60 on page 40
- **DHCP option 132**. section 18.4 DHCP Settings for Option 132 on page 41.
- configuration files: normally in **aastra.cfg** but it is also possible in **<model>.cfg** and in **<mac>.cfg.** The parameters are *tagging enabled* and *vlan id.*
- Phone UI. Touch **tools** > **terminal identity** > **advanced** > **useVLAN.**

The precedence is as in the list above.

12.4 Configuring Language Settings

It is only possible to set the display language via the configuration file (normally **8000i.cfg**/BluStar for Conference Room). The end user cannot select language.

If the language shall be changed, it must be changed in the configuration file with the parameter **language name**.

The following languages are at present available in this phone:

- English (default)
- French
- French Canadian
- German
- Italian
- Japanese
- Simplified Chinese
- Spanish
- Spanish Mexican
- Dutch

12.5 Authentication code

When entering a service code procedure containing an authorization or PIN code, it is not possible to replace the digits with stars in the display and in the logs.

12.6 Follow-me / Call Forward

It is possible to activate follow-me / call forward from the Telephone Feature Control area on the screen. Both external and internal follow me can be enabled.

The follow-me number must be set, otherwise the forward softkey is greyed out. Touch the following to set the number:
app menu > tools > call handling > call forward all

The extension must have a certain category to be allowed to activate follow-me.

The follow-me feature is executed in the system and not locally in the phone.

The necessary settings are described in 8.1 Installing aastra.cfg and 8000i.cfg configuration files on page 14.

12.7 Do Not Disturb (DND)

It is possible to activate individual DND from the Telephone Feature Control area on the screen.

The extension must have a certain category to be allowed to activate individual DND. When this feature is activated the forwarding of calls to the extension is dependant on the settings in MX-ONE.

The necessary settings are described in 8.1 Installing aastra.cfg and 8000i.cfg configuration files on page 14.

also MX-ONE Telephony System Feature List.

It is possible to activate group do not disturb from the telephone with a service code procedure. The extension must have a certain category to be allowed to activate group DND. No settings in the telephone is necessary for this feature. also MX-ONE Telephony System Feature List.

12.8 Using DNS SRV Resource Records

DNS SRV resource records cannot be used to implement redundancy in this release of BluStar 8000i/BluStar for Conference Room.

12.9 Central Storage of User Specific Data

This feature means that all the personal settings for a user are stored in a file that is stored on a central server. When the user logs on to another BluStar 8000i phone or BluStar for Conference Room unit, the user data will be available.

In BluStar 8000i/BluStar for Conference Room the user data is stored in the **<user>_local.cfg** file. Examples of this type of data are: incoming call logs, redial list, speed dial, favorites, max. video bandwidth and the settings for the three applications clock, weather and stock information.

12.10 Configuring the Diffserv Parameter

For details about the Diffserv /TOS / QoS settings, Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

12.11 Selection of Transport Addresses (Port Numbers)

The table below shows the default port numbers. These are possible to change via the **aastra.cfg** file.

Table 3 UDP/TCP ports used by the phone

Type of signalling	Default	Comment
RTP	3000	The first media stream, uses 3000 and 3002. Second uses 3004 and 3006, etc.
SIP	5060	
http	80	when downloading configuration and firmware files

12.12 Registration Distribution

In MX-ONE there is a concept called HLR (Home Location Register) server. The phones shall as the main rule be registered in their home server.

BluStar Configuration handles this automatically. If BluStar configuration is not used and the **user.cfg** shall be manually created, the parameters **sip proxy ip** and **sip registrar ip**, shall be set to the IP address of the HLR server.

Aastra 8000i/BluStar for Conference Room has no support for the registration distribution feature in MX-ONE.

12.13 Redundancy

There is no support for backup proxy / registrar in this release of BluStar 8000i/BluStar for Conference Room.

12.14 Registration at Branch Offices

There is no support for backup proxy / registrar in this release of BluStar 8000i/BluStar for Conference Room.

12.15 Home Office Scenario

The home office scenario means access via a Session Boarder Controller (for example Ingate).

The authentication of the log on from the video phone cannot be done via BluStar Configuration in MTS, because it is not possible to reach MTS from outside.

One possibility is to use a separate local http/ftp server for storing all the configuration files including **<user>.cfg** and **<user>_local.cfg**, 8.3.2 Log on/off using an FTP or HTTP server on page 19. This server must also host the application files, csv directory files and pictures.

The address to the http/ftp server must be configured manually in the BluStar 8000i phone/BluStar for Conference Room unit.

The IP address to the Session Boarder Controller is defined in the parameter *sip outbound proxy* in **aastra.cfg** or in **8000i.cfg/8000icr.cfg**.

12.16 Directories and Contacts

The BluStar 8000i/BluStar for Conference Room has the following directory and contacts functions:

- **Global directory**. It is a comma separated value (csv) file created by the system administrator. Access via the directory key on the BluStar 8000i/BluStar for Conference Room screen. The file name shall be **<name>.csv** and it shall be specified in the configuration file (normally in 8000i.cfg/8000icr.cfg) with the parameter **directory 1**.
- **LDAP directory**. Access also via the directory key on the BluStar 8000i /BluStar for Conference Room screen. The settings necessary for LDAP (Active Directory) can be defined in the 8000i.cfg /8000icr.cfg file. section 8.1.2 Manual handling of 8000i.cfg and aastra.cfg on page 14.

  When CMG directory is used, the transcoding from ISO-8859-1 to UTF-8 must be enabled in the 8000i.cfg file.
- **User directory**, also called contacts or address book. Access via the contacts key on the BluStar 8000i/BluStar for Conference Room screen. The contacts can be either:
  - A comma separated value (csv) file. The empty file, **<user>.csv**, is created by the system administrator and it is populated by the user. The directory file is specified in the user.cfg with the parameter **directory 2**.
  - The user's Microsoft Exchange® 2003 or 2007 SP1 (or later) contacts. If the user shall be allowed to download his Microsoft Exchange® personal contacts, this has to enabled in the 8000i.cfg/8000icr.cfg file. The configuration is done from the menus in the phone.

For a description of the parameter settings in the 8000i.cfg/800icr.cfg file, 8.1 Installing aastra.cfg and 8000i.cfg configuration files on page 14.

For more detailed information about the directory features, Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

12.17 Conference

The BluStar 8000i/BluStar for Conference Room supports conference calls of up to four participants, including the host. The terminal that initiates the conference becomes the conference leader and is responsible for all coordination between conference participants.

MX-ONE do not handle the video conference, instead it is the BluStar 8000i or the BluStar for Conference Room that is hosting and managing the conferences.

12.18 Call Park Pool

For a detailed description of the Call Park Pool feature in an MX-ONE environment, operational directions for Call Park Pool.

BluStar 8000i/BluStar for Conference Room cannot pickup a parked call from an MNS key.

12.19 SCA

There is no support for this feature when using the phone with the current MX-ONE release.

12.20 Extra Directory Number (EDN)

There is no support for this feature in this telephone.

12.21 MNS (BLF)

Monitoring of other extension numbers (MNS or BLF) can be done from the Aastra BluStar phone.

The extension number to be monitored in the BluStar 8000i phones or BluStar for Conference Room units must be initiated in MX-ONE or via Manager Provisioning as a MNS key. It must **also** be manually initiated in the BluStar 8000i phone/BluStar for Conference untit by initiating the favorite contact with the extension number of the monitored phone.

Note: The monitored number in the favorite contact must be the extension number. It cannot be an external number for example + 46 8 56867609.

To enable pick up of calls, the parameters for call pickup must be set in the **user.cfg** file.

Note: It is not possible to pick up parked calls with the Favorite key.

The BluStar devices are fully interoperable with the BluStar Server. By defining presence server and user details, the BluStar

devices will be able to take advantage of the enhanced presence capabilities offered by the BluStar Server.

The BluStar Server aggregates presence information from multiple sources and relays the information to the BluStar devices. BluStar device users are able to monitor the status for any contacts connected to the BluStar Server through their Favorites, Search, Contacts, History, and Directory menus as well as obtain more detailed status information through an individual's partial contact information display or full contact information page. Status information available in the various menus and pages include:

-Presence status bars and information (default as well as personalized status text).

-Line state details.

-Microsoft Exchange calendar activity.

Notes:

-At a minimum, the "sip presence server" and "sip presence user name" (including a valid e-mail address) must be defined in the phones/units configuration files to enable this feature.

-When the parameters are defined, the BluStar device will no longer send SUBCRIBE messages for the Busy Lamp Field (BLF) feature. Thus you will have either BluStar Presence OR MNS/BLF.

12.22 Solidus eCare

BluStar 8000i and BluStar for Conference Room can both be used as an agent with Solidus eCare.

12.23 Power Saving

The BluStar 8000i and BluStar for Conference Room integrates a power saving Eco-Off mode. Administrators can enable Eco-Off mode by defining the BluStar 8000i/BluStar for Conference Room user's normal operating work schedule. During the period of time outside of the specified work schedule, the BluStar 8000i/BluStar for Conference Room will automatically power down all extraneous hardware components and a screen saver will be initialized, thereby allowing for a reduction in overall energy consumption.

Users can also directly enable the Eco-Off power saving mode on the

BluStar 8000i/BluStar for Conference Room by selecting the **Eco-Off** button located in the Applications and Telephone Connection Management area of the screen.

User can ‘wake up’ the BluStar 8000i/BluStar for Conference Room while in Eco-Off mode by either touching the screen, pressing any hard key or lifting the handset.

All incoming calls will be ignored by the BluStar 800i/BluStar for Conference Room if it is in Eco-Off mode (i.e. a 480 temporarily unavailable response will be sent to the caller’s device).

Note: In a MX-ONE environment the recommendation is to disable the possibility for the end-user to program the Eco-Off mode schedule, example below.

Below is an example showing the Eco-Off mode schedule parameters in the 8000i.cfg/8000icr.cfg configuration file:

user defined power savings schedule:0
working monday:1
working tuesday:1
working wednesday:1
working thursday:1
working friday:1
working saturday:0
working sunday:0
working all days:0
working hour weekday start:06
working minute weekday start:00
working hour weekday end: 20
working minute weekday end:00
working hour weekend start:09
working minute weekend start:00
working hour weekend end:17
working minute weekend end:00
weekend working same as weekdays:0

In this example the user is not allowed to program power savings schedule, the terminal will be in normal operation Monday-Friday 06:00 to 20:00, Saturday-Sunday 09:00 to 17:00.

For a more detailed description of the settings in the phone, Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide

13 Passwords and PIN Codes

8.3 Log on / Log off on page 18.

14 Headset

Headset can be used with 8000i. For more information User Guide for Aastra BluStar 8000i Desktop Media Phone.

15 Expansion Modules

There are no support for expansion modules.

16 Emergency Calls

If the telephone is not registered to the PBX, it is not possible to make emergency calls.

17 Quality of Service (QoS)

For details about the Diffserv /TOS / QoS settings, Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.

It is not possible to view the QoS statistics via MX-ONE.

18 DHCP server

18.1 Data from DHCP

The phone has support for DHCP by which the following IP configuration data can be provided:

- Own IP address, subnet mask, default gateway and DNS, received in the DHCP standard fields (1 and 3).
- IP address to the software server. The path to the firmware to be downloaded from the software server can also be provided as well as the protocol to be used. The recommendation is to use DHCP option 66 (TFTP server name), but DHCP option 60 (vendor class identifier) and option 43 (vendor specific information field) can also be used.

The following example shows the different possibilities to use option 43 and option 66 to get the IP address and path to the software server:

http://192.168.1.45

http://192.168.1.45/path

http://httpsrv.example.com/path

If the phone receives the software server configuration in both option 66 and option 43, then option 43 takes precedence over option 66.

18.2 DHCP Settings for Option 66

Enter the URL to the software server according to the example in 18.1 Data from DHCP on page 40.

18.3 DHCP Settings for Option 43 and 60

DHCP option 60 (vendor class identifier) and option 43 (vendor specific information field) can also be used to get the software server address and also to load a unique configuration file dependant on telephone type.

The first step is to initiate option 60 for BluStar 8000i/BluStar for Conference Room:

Table 4 Identifier value to be defined in option 60

Model	Identifier Value
8000i	AastraBluStar8000i
8000icr	BluStarforConferenceRoom

After option 60 has been entered into the DHCP server, the data in option 43 has to be entered. The following options exist:

Table 5 Options that can be set in option 43.

Code	Description
02	Configuration server (protocol, server and path). Syntax: string
03	RCS. Not used in a MX-ONE environment
08	ID string to enable the use of the VLAN identity in code 09. Must be specified to avoid conflict with other vendors. Syntax: 16 bytes character string “Aastra(space)Telecom(space)(space)” i. e. 41617374726120546565636f6d2020
09	VLAN identity (1-4094) Syntax: 4 bytes whereas the first and second byte must be 0x00 and third and fourth byte the VLAN id. Example: 100 in decimal is 00 00 00 64 in hex.

For an example how to configure option 60 and 43 in a Linux environment, the Administrator Guide for Aastra IP SIP Phones

For an example how to configure DHCP in a Windows environment, installation instructions for Aastra 6700i SIP Terminals for MX-ONE.

18.4 DHCP Settings for Option 132

Option 132 provides the same VLAN functionality as option 43 and the data format of the VLAN identity is identical to the format listed in option 43 sub-option 09 in the table above.

For more information about VLAN priorities, section 12.3 Using Virtual LAN (VLAN) on page 27.

To enable option 132 a parameter in the configuration file has to be set (it is disabled by default):

dhcp option 132 vlan id enabled: 1

19 Security

SIP signaling with TLS and SRTP is supported for 8000i and BluStar for Conference Room.

To enable TLS and SRTP there are a number of parameters to be set in the configuration file, *Installation Instructions for Aastra 6700i SIP Terminals for MX-ONE*.

19.1 Encrypted Configuration Files

It is possible to store encrypted configuration files on the software server to protect against unauthorized access and tampering of sensitive information (e.g. user accounts, login passwords, registration information).

The system administrator uses a password distribution scheme to manually pre-configure or automatically configure the terminals to use the encrypted configuration with a unique key.

From a Microsoft Windows command line, the administrator uses an Aastra-supplied encryption tool called "anacrypt.exe" to encrypt the configuration files.

The anacrtypt tool can be downloaded from Aastra Service Plaza.

This tool is also available for a Linux platform i. e. anacrypt.linux.

Note: The current version of MTS cannot handle encrypted configuration files. If this function shall be used, the configuration files have to be created manually outside MTS.

19.1.1 Description of the Encryption

The anacrypt tool processes the plain text <user>.cfg, <user>_local.cfg, <mac>.cfg, <model>.cfg, and aastra.cfg files and creates triple-DES encrypted versions called <user>.tuz, <user>_local.tuz, <mac>.tuz, <model>.tuz, and aastra.tuz.

Encryption is performed using a secret password (4-32 alphanumeric characters) that is chosen by the administrator.

The encryption tool is also used to create an additional encrypted tag file called security.tuz, which controls the decryption process on the BluStar 8000i/Blustar for Conference Room. If security.tuz is present on the system configuration server during the boot up sequence, the BluStar 8000i/BluStar for Conference Room downloads it and uses it

locally to decrypt the configuration information from the aastra.tuz, <model>.tuz and <mac>.tuz files (as well as the <user>.tuz and <user>_local.tuz files if they are located on the same server).

If the <user>.tuz and <user>_local.tuz files are located on a separate user configuration server, and a security.tuz file is present on this separate server during a user login or check-sync, the BluStar 8000i downloads it and uses it locally to decrypt the configuration information from the <user>.tuz and <user>_local.tuz files. Security.tuz is also used by the phone to encrypt **<user>.tuz** and **<user>_local.tuz.**

19.1.2 Procedure for Encryption

The procedure for encryption of configuration files is:

- Open a command line window application (i.e., DOS window).
- At the prompt, enter anacrypt.exe and press <Return>
- Enter a command utilizing the details provided in the help screen.

Syntax:

```
anacrypt {infile.cfg|-d <dir>} [-p password] [-m] [-i] [-v] [-h]
m = Generate <mac>.tuz files that are terminal specific
i = Generate security.tuz file
v = Specifies the encryption key version (options include -v1 and
-v2 [default])
h = Show the help screen
```

Example 1

Generating a security.tuz file with password 1234abcd using the v2 encryption key.

```
C:\>anacrypt -i -p 1234abcd -v2
```

Example 2

Encrypting a single aastra.cfg file with password 1234abcd

```
C:\>anacrypt aastra.cfg -p 1234abcd
```

Example 3

Encrypting all cfg files in C:\data with password 1234abcd using MAC encryption and generating a security.tuz file at the

same time.

C:\>anacrypt -d C:\data -p 1234abcd -m -i

20 Troubleshooting

There is support for log files for trouble shooting.

The system administrator can enable parameters in the aastra.cfg or 8000i.cfg/8000icr.cfg files for the following options:

- Syslog location
- System-wide logging
- SIP stack logging
- Debug logging.

For a detailed description of the parameters, Aastra BluStar 8000i Desktop Media Phone/BluStar for Conference Room, SIP Call Server Administrator Guide.